

Original citation:

Rejeb, Ridha, Leeson, Mark S. and Green, Roger. (2006) Fault and attack management in all-optical networks. IEEE Communications Magazine, 44 (11). pp. 79-86.

Permanent WRAP URL:

<http://wrap.warwick.ac.uk/32818>

Copyright and reuse:

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions. Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

Publisher's statement:

"© 2006 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting /republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works."

A note on versions:

The version presented here may differ from the published version or, version of record, if you wish to cite this item you are advised to consult the publisher's version. Please see the 'permanent WRAP URL' above for details on accessing the published version and note that access may require a subscription.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk

Fault and Attack Management in All-Optical Networks

R. Rejeb, M. S. Leeson, and R. J. Green, *University of Warwick, UK*

Abstract— Network management for optical networks faces additional security challenges that arise by using transparent optical network components in communication systems. Whilst some of available management mechanisms are applicable to different types of network architectures, many of these are not adequate for all-optical networks. These have unique features and requirements in terms of security and quality of service thus requiring a much more targeted approach in terms of network management. In this paper we consider management issues with particular emphasis on complications that arise due to the unique characteristics and peculiar behaviors of transparent network components. In particular, signal quality monitoring is still a major complication in all-optical networks. Despite new methods for detection and localization of attacks having been proposed, no robust standards or techniques exist to date for guaranteeing the quality of service in these networks. Therefore, the need for more sophisticated mechanisms that assist managing and assessing the proper function of transparent network components is highly desirable. Accordingly, we present an algorithm for multiple attack localization and identification that can participate in some tasks for fault management of all-optical networks.

Index Terms—All-Optical Networks, Fault Management, Optical crosstalk, Optical Network Security.

I. INTRODUCTION

NETWORK management is an indispensable constituent of communication systems since it is responsible for ensuring the secure and continuous functioning of any network. Specifically, a network management implementation should be capable of handling the configuration, fault, performance, security, and accounting in the network. Whilst some of available management mechanisms are applicable to different types of network architectures, many of these are not adequate for All-Optical Networks (AONs). These contain only transparent optical components and therefore differ to a large extent from the optical networks currently used. As a result, AONs have unique features and requirements in terms of security and Quality of Service (QoS) that require a very targeted approach in terms of network management. Although the job of network management for AONs is essentially no different from that of managing traditional optical networks, numerous management issues arise, in particular because of network transparency and the characteristics of AON

components. These specific features thus require more sophisticated techniques and methods for managing and monitoring the network, controlled with an appropriate Network Management System (NMS) that can meet and satisfy the challenges posed by AONs [1].

In this paper we consider management issues that arise by using AON components in communication systems. First, we provide a brief overview of faults and attacks that may occur in AONs. Next, we focus on management issues with particular emphasis on complications that arise due to the unique characteristics and peculiar behaviors of various AON components. Then, we present the key concepts of an algorithm for multiple attack localization and identification that can be used in some tasks for fault management of AONs.

II. FAULTS AND ATTACKS IN AONs

AONs offer the promise of increased capacity, flexibility, and scalability, compared to the optical networks currently in use. In particular, they provide transparency capabilities and new features, allowing routing and switching of traffic without any examination or modification of signals within the network. Although transparency offers many advantages for high data rate communications, it brings forth a set of new challenges in terms of network security, which do not exist in traditional networks [2]. One of the serious problems with network transparency is that the properties of transparent optical components make AONs particularly vulnerable to various forms of service disruption, QoS degradation, and eavesdropping attacks. A problem that comes up in this regard is that network transparency may introduce significant miscellaneous transmission impairments, which range from simple attenuation to complex non-linear effects and polarization dependent losses. This raises the danger that those impairments will aggregate and become significant as the signal traverses successive nodes, imposing component-crosstalk constraints that tighten rapidly as the network grows in size. Another problem related to transparency is that accumulated transmission impairments and service disruption attacks spread rapidly through the network. Specifically, if the traffic itself is the cause of the failure, multiple failures will be caused throughout the network and propagate quickly without any restoration. In this case, the extremely high data rates in AONs ensure that, even if the network were under attack for a few seconds, large amounts of data to be lost or compromised. This in particular makes detection and identification of attacks a crucial task for fault management, since these attacks can be

Manuscript received March 17, 2005.

Dr. R. Rejeb, University of Warwick, (ridha.rejeb@iaer.eu)

Dr. M. S. Leeson, University of Warwick, (mark.leeson@warwick.ac.uk)

Prof. R. J. Green, University of Warwick, (roger.green@warwick.ac.uk)

launched elsewhere in the network eluding most available monitoring techniques. These methods are in general not sensitive enough to detect small and sporadic bit error rate (BER) degradations [2]. Carefully addressing these issues requires, therefore, a comprehensive understanding of the unique characteristics of AON components that make possible the distinguishing of attacks from conventional failures.

A. Type of Attacks in AONs

Security attacks upon AONs may range from a simple physical access to more complex attacks exploiting: a) the peculiar behaviours of optical fibers, b) the unique characteristics of AON components, and c) the shortcomings of available supervisory techniques [3]. However, attacks can be considered from different viewpoints. From an attacker's perspective, attacks can be broadly categorized into six areas: traffic analysis, eavesdropping, data delay, service denial, QoS degradation, and spoofing [2]. Since some of these areas may have similar characteristics, attacks can be broadly grouped into two main categories, namely service disruption and eavesdropping, which may be achieved by gaining access to the network through authorized or unauthorized entry points. However, to realize a disruption attack, an attacker that can gain access to the network may implement, for example, an *in-band* or *out-band* jamming attack method. To implement the former method, the attacker can take advantage of the unique characteristics of AON components such as the gain saturation of optical amplifiers. The attacker can gradually increase the power of one channel with respect to the other copropagating channels at the input of an optical amplifier so that the output of some channels may be too low or too high. As a consequence of not having adequate measures to detect and report on its abnormal power intensity, the attacking signal will propagate through the network as if it were a legitimate user, and significantly deprive other legal channels of their gains along its route. In particular when the attacking signal gets strong enough, the affected channels may suffer from performance degradation that produces a complete loss of service. Similarly, to implement an out-of-band jamming attack, the attacker may insert power at a wavelength outside the signal window and cause thereby transmission effects such as the Raman effect¹ to degrade the signal quality of copropagating channels. Unlike performing an eavesdropping attack, which can be achieved by an unauthorized observation method, the attacker attempts to gain information from adjacent signals making use of crosstalk leaking from shared network resources.

From a management perspective, security failures and attacks upon AONs may be also considered based on their specific characteristics and attributes such as the attack methods used, attack access points as well as the AON components and transmission segments targeted. Attacks can be broadly classified into two main types namely *direct attacks* and *indirect attacks* [4]. The former are more related to physical network components and can be directly

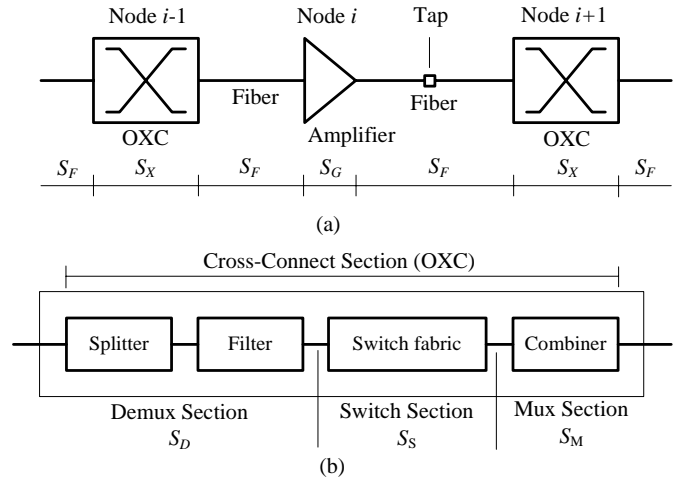


Figure 1. Management sections. (a) Sequence of management sections along an optical link segment. (b) Management sections into an OXC node.

implemented on different AON components such as taps and optical fibers. In contrast, the latter are unlikely to be performed directly or their entry points are not easily accessible to potential attackers. In this case, an attacker attempts to use indirect means, taking advantage of possible vulnerabilities of AON components and other transmission effects (for example crosstalk effects) to gain access to the network. In comparison to direct attacks, which are in general easier to detect and rectify, indirect attacks require expert diagnostic techniques and more sophisticated management mechanisms to ensure the secure and proper function of the network. However, either type of these attacks may be targeted at three major AON components, namely optical fiber cables, optical amplifiers, and switching nodes. As illustrated in Figure 1 (a), these components can be modeled as a sequence of interrelated *management sections* [4]. A typical transmission segment may be divided in three sections: Fiber Section (S_F), Gain Section (S_G), and Cross-Connect (OXC) Section (S_X). As illustrated in Figure 1 (b), the management section S_X can be in turn subdivided into three additional sections namely Demultiplexer Section (S_D), Switching Section (S_S), and Multiplexer Section (S_M). Table I summarizes the common known types of attacks that may be practiced upon these management sections.

To illustrate how attacks interact with each other as they propagate through the network, we now consider an attack scenario that may occur along a typical transmission segment. Figure 2 shows a sample OXC node with two input and output fibers supporting two wavelength channels. An attacker that

TABLE I
ATTACK TYPES AND METHODS IN AONs.

Attack type	Attack method	Component	Section
Service Disruption	In-band jamming power	Fiber	S _F
	Out-band jamming power	Fiber	S _F
	Intentional crosstalk	Splitter	S _D
		Filter	S _D
		Switch	S _S
		Combiner	S _M
Eavesdropping	Unauthorized observation	Amplifier	S _G
		Fiber	S _F
		Tap	S _F

¹ Raman effect or stimulated Raman scattering is one of the non-linear effects that can be used to degrade the quality of optical signals.

can gain access to the network as shown in Figure 2 (a), is then able to perform a service disruptive attack by injecting a strong optical signal at wavelength λ_2 , which is already in use. This causes an increase of the optical power at that wavelength and can thus impact other legitimate channels that copropagate at the same time. When traversing the optical amplifier (gain section S_G), shown in Figure 2 (b), channel λ_2 robs channel λ_1 of power and propagates downstream through successive AON components, affecting other legal channels along its route. This type of attack is known as a *gain competition attack*. Further, the demultiplexers, Figure 2 (c) and (g), ideally separate incoming wavelengths to corresponding switches. The nonideal crosstalk specification of the optical demultiplexer means that a small portion of the signal at channel λ_1 leaks into the adjacent channel λ_2 and vice versa. When passing through the optical switches (section S_S), Figure 2 (d) and (h), channels with the same wavelength interfere with each other. This causes crosstalk arising from the nonideal isolation of one switch port from the other. As shown in Figure 2 (e) and (i), when the channels are combined again by the multiplexer, a small portion of λ_1 that leaked into λ_2 will also leak back into the common output fiber. This also causes crosstalk, which accumulates from several AON components as the signals propagate downstream through many intermediate AON nodes in the network. According to whether it has the same nominal wavelength as an affected signal or not, crosstalk can be categorized in two forms, namely *interchannel crosstalk* and *intrachannel crosstalk* [5]. The former arises between adjacent signals at different wavelengths, whilst the latter occurs between signals at the same nominal wavelength. Both forms of crosstalk can arise from a variety of sources. Compared to interchannel crosstalk, intrachannel crosstalk effects are of prime importance for AONs because they can lead to severe power penalties and cannot be eliminated by the optical filters or demultiplexers. Intrachannel crosstalk thus imposes an important limitation on practical implementation of AONs.

B. Failures versus Attacks

Conventional component failures in AONs usually occur because of malfunctions or breakdowns of AON devices and components. Examples include optical fiber cuts, loss of light, lightpath failures, and fuse or power circuit disruptions. Although AON components have fairly long *mean-time-between-failures* (typically several years), they may fail due to the physical natural fatigue and ageing of component

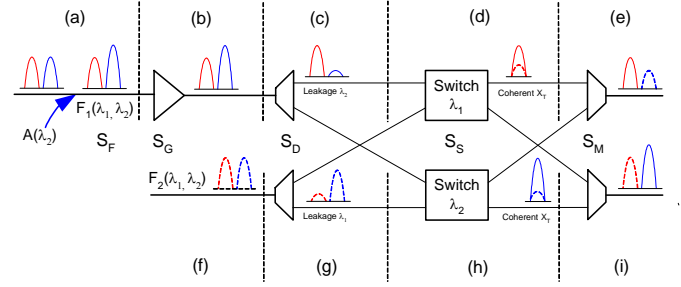


Figure 2. An attack propagation scenario. The attack propagates through a link segment passing through an optical amplifier, wavelength demultiplexer, optical space switch, and wavelength demultiplexer.

constituents [6]. Another source of failure arises from bandwidth narrowing due to the cascading of filters, and wavelength misalignment between multiplexers and demultiplexers. Failures in optical amplifiers occur from a variety of sources such as loss of light or failing of passive components within the amplifier. However, these failures are in general easier to detect and rectify using standard localizing metrology as means for monitoring, detecting, and isolation methods. Upon detection, these failures are immediately communicated as single alarms to the NMS that will establish appropriate protection and restoration reactions in accordance with the facts.

In contrast, security attacks differ substantially from conventional failures and should be therefore treated differently. This is because attacks appear and disappear sporadically and can be launched elsewhere in the network. In particular, the attacker may thwart simple detection methods, which are in general not sensitive enough to detect small and sporadic performance degradations. Furthermore a disruptive attack, which is erroneously identified as a component failure, can spread rapidly through the network causing additional failures and triggering multiple alarms. Consequently, rerouting of traffic cannot solve all resulting failures and problems, as is the case of component failures. Table II provides a comparison of conventional failures versus disruption attacks that may be practiced upon AONs.

III. AVAILABLE SUPERVISORY AND MONITORING METHODS

Fault management functions may be broadly classified into three categories: (a) prevention; (b) detection; (c) reaction. Fault detection deals with detecting and isolating failures when they occur, and also includes alarm generation. Fault protection and restoration refers to the processes used to guard against failed conditions and to restore network services in the event of transmission failures. In protecting optical networks,

TABLE II
COMPARISON OF CONVENTIONAL FAILURES VERSUS DISRUPTION ATTACKS IN AONs.

Characteristics	Failures	Attacks
Behaviors	<ul style="list-style-type: none"> - occur slower than attacks due to physical natural fatigue and ageing of optical devices and components. - occur once and remain disabled until they are repaired again. - do not disturb the operation of several devices at the same time. - lead to single alarms. 	<ul style="list-style-type: none"> - appear and disappear often sporadically in the network. - spread rapidly through the network without restoration. - elude most of available supervisory techniques. - cause additional failures and problems in the network. - trigger multiple erroneous and undesirable alarms.
Identification and detection methods	<ul style="list-style-type: none"> - rely on identifying the domain of raised alarm and correlating the failures using algorithms and statistical methods to determine the likelihood of certain failures having occurred. 	<ul style="list-style-type: none"> - used methods vary from simple to more complex. - using diagnostic, electronic and photonic methods.
Restoration schemes	<ul style="list-style-type: none"> - rerouting of traffic channels can solve all resulting problems. 	<ul style="list-style-type: none"> - rerouting of traffic cannot solve all resulting problems.
Occurrence sections	<ul style="list-style-type: none"> - usually within optical devices and components. 	<ul style="list-style-type: none"> - can launch elsewhere in the network.

TABLE III
FAILURE DETECTION CAPABILITIES OF AVAILABLE SUPERVISORY AND MONITORING METHODS

Supervisory and Monitoring Techniques	Signal Domain	In-Band Jamming	Out-Band Jamming	Time Distortion	Noise	Accuracy
BER measurements	Digital	Yes	Yes	Yes	Yes	High
Sampling methods	Optical	Yes	Yes	Yes	Yes	Medium
Optical Power Meters	Optical	No	No	No	No	Low
BER Testers	Optical	No	No	No	No	Low
Optical Spectral Analyzers	Optical	No	Yes	No	No	Low
Pilot tones	Optical	No	No	No	No	Low
Optical Time Domain Reflectometers	Optical	No	No	No	No	Low
Optical Frequency Domain Reflectometers	Optical	Yes	Yes	No	No	Medium

supervisory techniques are required, enabling the detection of failures, and these may currently be grouped into two categories [2]. The first is based on methods that perform statistical analysis of the transmitted data: power detection, optical spectral analyzers and BER testers. The second relies on the use of probe signals devoted to diagnostic purposes: pilot tones and optical time domain reflectometers. However, most of these supervisory techniques are insufficient to detect small and sporadic BER degradations, failing to detect in-band and out-of-band jamming attacks. Even the use of probe signals is not sensitive enough to detect BER degradations.

Recent proposals to overcome the difficulty of determining the continuity and quality of optical signals include error detecting codes, sampling and spectral methods. However most of these methods are too difficult to implement in every AON component or require the access to the electrical domain. Table III summarizes fault detection capabilities of available monitoring methods. Regarding cost, complexity, and implementation plausibility, these methods may be listed in decreasing order of difficulty and also decreasing information content as follows [3]:

1. *BER estimation with access to digital signal* – BER measurement methods.
2. *BER estimation with access to optical signal* – Sampling methods (Eye monitoring).
3. *Power and noise monitoring* - optical signal-to-noise ratio.
4. *Indirect methods* – are methods that do not directly sense the signal shape or power but still indicate the proper function of network components.

The conclusion is that the problems rising from physical security in AONs and the means of protecting against them cannot be tackled using current available supervisory and monitoring techniques. Despite new methods for detection and localization of security attacks having been proposed, no robust standards or techniques exist to date for guaranteeing the quality of service in AONs.

IV. MANAGEMENT ISSUES

Following from the previous sections, it is clear that network management for AONs faces additional challenges and still unsolved problems. One of the main premises of AONs is the establishment of a robust and flexible optical control plane for managing network resources, provisioning and maintaining network connections across multiple control domains. Such a control plane must have the ability to select

lightpaths² for requested *end-to-end* connections, assign wavelengths to these lightpaths, and configure the appropriate optical resources in the network. Furthermore, it should be able to provide updates for link state information to reflect which wavelengths are currently being used on which fiber links so that routers and switches may make informed routing decisions. An important issue that arises in this regard is how to address the *trade-off* between service quality and resource utilization. Addressing this issue requires different scheduling and sharing mechanisms to maximize resource utilization while ensuring adequate QoS guarantees. One possible solution is the aggregation of traffic flows to maximize the optical throughput and to reduce operational and capital costs.

Another related issue arises from the fact that the implementation of a control plane requires information exchange between control and management entities that are involved in the control process. To achieve this, fast signaling channels need to be in place between switching and routing nodes. These channels might be used to exchange *up-to-date* control information that is needed for managing all supported connections and performing other control functions. In general, control channels can be realized in different ways; one might be implemented in-band while another may be implemented out-of-band. There are, however, compelling reasons for decoupling control channels from their associated data links. An important reason for this is that data traffic carried in the optical domain is transparently switched to increase the efficiency of the network and there is thus no need for switching nodes to have any understanding of the protocol stacks used for handling the control information. Another reason is that there may not be any active channels available while the data links are still in use, for example when bringing one or more control channels down gracefully for maintenance purposes. From a management point of view, it is unacceptable to tear down a data traffic link, simply because the control channel is no longer available. Moreover, between a pair of switching nodes there may be multiple data links and it is therefore more efficient to manage these as a bundle using a single separated out-of-band control channel.

In recent years, the notion of an optical control plane has received extensive attention and has rapidly developed to a detailed set of protocol standards, currently being standardized by the International Telecommunication Union-

² A lightpath is defined as an *end-to-end* optical connection between a source and a destination transparent node.

Telecommunication Standardization Sector and others [7]. Nevertheless, several additional issues in terms of security and network management are still unsolved [1]-[4]. One of the main management issues revolves around the fact that very little is currently understood concerning performance monitoring in AONs. For example, when discussing routing in AONs, it is usually assumed that all routes have adequate signal quality (ensured by limiting AONs to sub-networks of limited size). This approach is very practical and has been applied to date when determining the maximum length of optical links and spans, for example. In addition, operational considerations such as failure isolation also make limiting the size of domains of transparency very attractive.

Performance management is still a major complication in AONs, since optical performance measurements, which are typically limited to optical power, Optical Signal-to-Noise Ratio (OSNR), and wavelength registration, do not directly relate to QoS measures used by carriers. These are concerned with attributes related to the lightpath, such as BER and parity checks, of which the management system may have no prior knowledge. Moreover, transparency means that it is not possible to access overhead bits in the transmitted data to obtain performance-related measures, adding further complexity to the detection of service disruption. Unless information concerning the type of signal that is being carried on a lightpath is conveyed to the NMS, it will not be able to ascertain whether the measured power levels and OSNR fall within the preset acceptable limits.

Fault management is further complicated since detection functions, which should be handled at the ISO layer closest to the failure, are delegated to the physical layer instead of higher layers. That is, fault detection and localization methods are less insulated from details of physical layer than of higher layers, requiring the availability of expert diagnostic techniques to measure and control the smallest granular component, the wavelength channel. Moreover, security failure identification of both the location and type of attacks differs significantly from that in traditional networks, which basically relies on identifying the domain of an alarm and using algorithms to determine the probability of a certain failure having occurred. Although the same techniques can be applied to AONs, several issues exist and need to be addressed carefully [1]-[4].

V. ATTACK LOCALIZATION AND IDENTIFICATION ALGORITHM

This section presents an outline of the Multiple Attack Localization and Identification (MALI) algorithm [5] that can participate in some tasks for fault management of AONs. The main task of the MALI algorithm is to correlate multiple security failures and attacks locally at any AON node and to discover their tracks through the network. The MALI algorithm is distributed and relies on a reliable management system such as the Link Management Protocol [8], since its overall success depends upon correct message passing and processing at the local nodes.

The key concepts of the MALI algorithm are based on the

OXC node model proposed in [5]. This model defines an OXC node as a 7-tuple $OXC = (F, W, D, S, M, \chi, \mu)$, where F , W , D , S , and M are nonempty component sets of fiber ports, supported wavelengths, wavelength demultiplexers, optical switches, and wavelength multiplexers, respectively. The main key functions of the OXC node model are represented by χ and μ . These are responsible for updating the connection and monitoring information of all established lightpaths that copropagate through the OXC node simultaneously. The model denotes the numbers of fiber ports and supported wavelengths by n and m , respectively. To identify the source and nature of detected performance degradation, the algorithm makes particular use of *up-to-date* connection and monitoring information of any established lightpath, on the input and output side of each node in the network. The required monitoring information and measurements can be correlated at local nodes or acquired from remote monitoring nodes [9].

The MALI algorithm mainly runs a generic localization procedure, which will be initiated at the downstream node that first detects serious performance degradation at an arbitrary lightpath on its output side.

A downstream node, which first notices serious performance degradation at a disturbed lightpath, raises an alarm, indicating that a failure is detected on its output side. Next, it computes the required channel state information on its input side. Then, it determines the set of lightpaths that share the same output fiber with the disturbed lightpath. For each of these, it determines the set of lightpaths that pass through the same optical switch at the same time. Hence, it delegates the localization process to next upstream node when the status of a lightpath channel is nonzero on the input side of the node. Otherwise, it terminates the localization process for this lightpath and notifies the NMS that the disturbed lightpath is most likely to be affected in the current node.

An upstream node that receives the localization process with a disturbed lightpath starts the localization procedure from scratch and repeats all steps when the channel status of the disturbed lightpath is nonzero on the output side of the node. Otherwise, it terminates the localization process and notifies the NMS indicating that the failure is most likely to be at the optical fiber link interconnecting both upstream and downstream nodes.

The localization procedure provides to the NMS information about locations of possible failures and attacks. The information can be included as part of the failure notifications. Once the origins of the detected failures have been localized, the NMS can then make an accurate decision (for example, which offender lightpaths should be disconnected or rerouted) to achieve finer grained recovery switching actions. However, the whole localization process can be solved in a linear time depending on the distribution of upstream nodes involved in the process [10].

Figure 3 shows an attack propagation scenario, where several OXC nodes are interconnected by optical fiber links. Each node consists of 2 fiber ports, 2 demultiplexer and multiplexer pairs, and 2 optical space switches. Seven

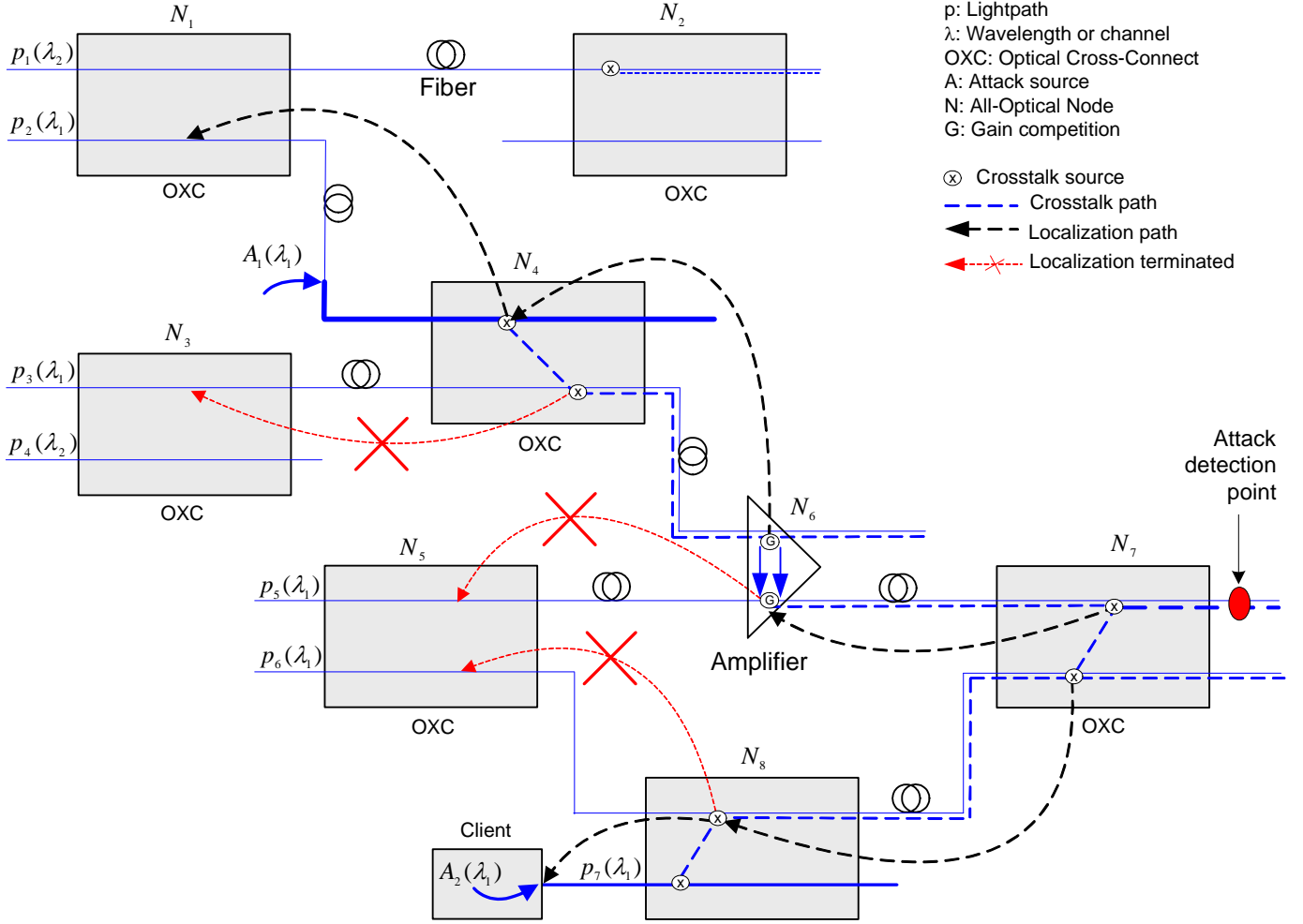


Figure 3: An attack propagation scenario. The sample network consists of 7 OXC nodes interconnected with each other by optical fiber links. Each node consists of 2 incoming/outgoing fiber pairs, 2 wavelength demultiplexer/multiplexer pairs, and 2 optical space switches. Seven lightpaths propagate through the network, simultaneously. The detected disruption at node N_7 stems from two different sources A_1 and A_2 , carried along with lightpaths p_2 and p_7 , respectively. Lightpath p_5 , on which serious performance degradation is detected, is innocent and should not be disconnected.

lightpaths, p_1 to p_7 , propagate through the network simultaneously. Performing the MALI algorithm leads to the following results: The detected performance degradation at node N_7 stems from two different sources and the offender lightpaths in this case are p_2 and p_7 . Lightpath p_2 is directly affected by a power jamming attack A_1 , which causes an increase of the optical power at that lightpath, and thus impacts copropagating lightpath p_3 as they pass through node N_4 . When traversing the optical amplifier (node N_6), lightpath p_3 robs lightpath p_5 of power (gain competition attack) and propagates downstream through successive transparent optical components, affecting other legal lightpaths along its route. On the other hand, lightpath p_7 , which is disturbed by a malicious attack A_2 , affects copropagating lightpath p_6 as they pass through node N_8 at the same time. When passing through node N_7 , lightpath p_6 , in turn, affects its neighboring lightpath p_5 . However, lightpath p_5 , on which serious performance degradation is

detected, is innocent and should not be disconnected. Since A_1 is a power jamming attack on the optical link $N_1 \rightarrow N_4$, the NMS may reroute lightpath p_2 thereby avoiding node N_4 . Lightpath p_7 , which added in node N_8 , should be immediately disconnected until attack A_2 is thoroughly isolated.

VI. CONCLUSION

Network management for AONs faces additional challenges such as performance monitoring and ensuring adequate QoS guarantees in the network. Performance management is germane to successful AON operation since it provides signal quality measurements at very low BERs and fault diagnostic support. In particular, signal quality monitoring is difficult in AONs as the analogue nature of optical signals means that miscellaneous transmission impairments aggregate and can impact the signal quality enough to reduce the QoS without precluding all network services. This results in the continuous monitoring and identification of the impairments becoming challenging in the event of transmission failures.

In this paper, we have discussed various management issues in AONs with particular emphasis on complications that arise from the unique characteristics and behaviors of AON components. A simple and reliable signal quality monitoring method does not exist at present. Therefore, the employment of additional approaches that rely on available mentoring methods is extremely useful for assessing the proper and secure functioning of AON components. Accordingly, we have presented an outline of our MALI algorithm, which can make a contribution to the fault management of AONs. The MALI algorithm offers the advantage of managing faults and attacks with less monitoring information than is required by other approaches. As a direct consequence, the algorithm reduces the cost and complexity of signal monitoring for future AON NMS solutions.

REFERENCES

- [1] R. Rejeb, I. Pavlosoglou, M. S. Leeson, and R. J. Green, "Management Issues In Transparent Optical Networks", *6th IEEE International Conference on Transparent Optical Networks*, vol. 1, pp. 248-254, Wroclaw, July 2004.
- [2] M. Medard, S. R. Chinn, and P. Saengudomlert. "Node wrappers for QoS monitoring in transparent optical nodes", *Journal of High Speed Networks*, vol. 10, no. 4, pp. 247-268, 2001.
- [3] C. P. Larsen, and P. O. Andersson, "Signal Quality Monitoring in Optical Networks", *Optical Networks Magazine*, vol. 1, no. 4, pp. 17-23, Oct. 2000.
- [4] J. K. Patel, S. U. Kim and D. H. Su, "Modeling Attack Problems and Protection Schemes for All-Optical Transport Networks", *Optical Networks Magazine*, vol. 3, no. 4, pp. 61-72, July/August 2002.
- [5] R. Rejeb, M. S. Leeson, and R. J. Green, "Multiple Attack Localization and Identification in All-Optical Networks", *Optical Switching and Networking*, vol. 3, no. 1, pp. 41-49, 2006.
- [6] C. Mas, I. Tomkos and O. K. Tonguz, "Optical networks security: a failure management framework", *ITCom, Optical Communications & Multimedia Networks*, Orlando, Florida, 7-11 September 2003.
- [7] D. Saha, B. Rajagopalan, and G. Bernstein, "The Optical Network Control Plane: State of the Standards and Deployment", *IEEE Optical Communications*, vol.1, no. 3, August 2003.
- [8] J. Lang, et al., "Link Management Protocol (LMP)", *Internet Draft*, Work In Progress, 2004.
- [9] T. Wu, A. K. Somani, "Necessary and Sufficient condition for k crosstalk attacks localization in All-Optical Networks", *Proceeding of IEEE Globecom 2003*, Dec. 1-5, 2003.
- [10] R. Rejeb, M. S. Leeson, and R. J. Green, "Fault Management In Transparent Optical Networks", *8th IEEE International Conference on Transparent Optical Networks*, vol. 3, pp. 143-148, Nottingham, 18-22 June, 2006.